

[19]中华人民共和国国家知识产权局

[51]Int. Cl⁷

G06F 9/48

H04L 9/00

[12] 发明专利申请公开说明书

[21] 申请号 01103000.3

[43]公开日 2001年8月22日

[11]公开号 CN 1309351A

[22]申请日 2001.2.14 [21]申请号 01103000.3

[30]优先权

[32]2000.2.14 [33]JP [31]035898/2000

[32]2000.5.8 [33]JP [31]135010/2000

[71]申请人 株式会社东芝

地址 日本神奈川县

[72]发明人 桥本干生 寺本圭一 齐藤健

白川健治 藤本谦作

[74]专利代理机构 中国国际贸易促进委员会专利商标事
务所

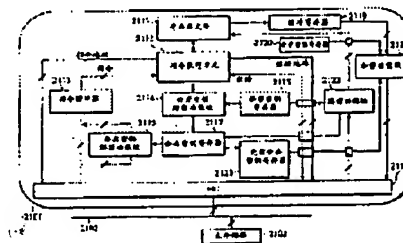
代理人 吴丽丽

权利要求书4页 说明书43页 附图页数15页

[54]发明名称 抗干预微处理器

[57]摘要

在多任务环境下,抗干预微处理器保存一个其执行被中断的程序的上下文信息,其中该上下文信息含有指明该程序的执行状态和该程序的执行码密钥的信息。通过从保存的上下文信息恢复该程序的执行状态,可以重新启动该程序的执行。利用微处理器的公开密钥可以将此上下文信息加密,然后利用微处理器的秘密密钥进行解密。





权 利 要 求 书

1. 一种具有不能被读出到外部的唯一秘密密钥和与该唯一秘密密钥对应的唯一公开密钥的微处理器，该微处理器包括：

读取单元，被进行配置以从外部存储器读出多个利用不同执行码密钥加密的程序；

解密单元，被进行配置以利用各自解密密钥，对多个通过读取单元读出的程序进行解密；

执行单元，被进行配置以执行多个利用解密单元解密的程序；

上下文信息保存单元，被进行配置以将其执行被中断的一个程序的上下文信息保存到外部存储器或保存到在微处理器内部设置的上下文信息存储器，该上下文信息含有指明此程序的执行状态和此程序的执行码密钥的信息；以及

重新启动单元，被进行配置以通过从外部存储器或上下文信息存储器读出上下文信息并通过从上下文信息中恢复此程序的执行状态，重新启动执行此程序。

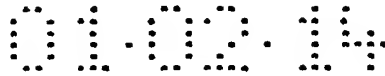
2. 根据权利要求 1 所述的微处理器，其中所配置的上下文信息保存单元利用公开密钥对上下文信息进行加密，并将加密上下文信息保存到外部存储器；以及

所配置的重新启动单元通过从外部存储器读出加密上下文信息，利用秘密密钥解密加密上下文信息，以及从解密上下文信息中恢复一个程序的执行状态，重新启动此程序的执行。

3. 根据权利要求 2 所述的微处理器，其中仅当包含在解密上下文信息内的解密执行码密钥与此程序的执行码密钥一致时，重新启动单元才重新启动此程序的执行。

4. 根据权利要求 2 所述的微处理器，其中重新启动单元将包含在解密上下文信息内的解密执行码密钥用作解密密钥以解密此程序。

5. 根据权利要求 1 所述的微处理器，其中所配置的上下文信息保存单元以明文形式将上下文信息保存到此程序被中断后所执行的另一



个程序不可读的上下文信息存储器; 以及

通过从上下文信息存储器读出上下文信息并从上下文信息恢复此程序的执行码, 所配置的重新启动单元重新启动此程序的执行。

6. 根据权利要求 5 所述的微处理器, 其中重新启动单元根据另一个程序规定的指令重新启动此程序的执行。

7. 根据权利要求 6 所述的微处理器, 其中在此程序的执行被中断时, 上下文信息保存单元将上下文信息保存到上下文信息存储器, 并利用公开密钥将上下文信息存储器内的上下文信息加密, 然后根据另一个程序规定的另一条指令的执行, 将加密上下文信息存储到外部存储器。

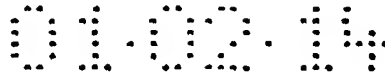
8. 根据权利要求 5 所述的微处理器, 其中在此程序的执行被中断时, 上下文信息保存单元将上下文信息保存到上下文信息存储器, 利用公开密钥将上下文信息存储器内的上下文信息加密, 然后将加密上下文信息存储到另一个程序规定的外部存储器。

9. 根据权利要求 1 所述的微处理器, 其中所配置的上下文信息保存单元产生作为临时密钥的随机数、加密上下文信息、然后将加密上下文信息存储到外部存储器, 加密上下文信息含有: 第一数值, 通过对信息进行加密获得, 利用临时密钥指明此程序的执行状态; 以及第二数值, 通过利用公开密钥加密临时密钥获得; 以及

通过从外部存储器读出加密上下文信息, 利用秘密密钥由包含在加密上下文信息内的第二数值解密获得临时密钥, 利用解密的临时密钥由包含在加密上下文信息内第一数值解密出指明执行状态的信息, 以及从解密上下文信息恢复此程序的执行状态, 所配置的重新启动单元重新启动此程序的执行。

10. 根据权利要求 9 所述的微处理器, 其中上下文信息保存单元保存还含有利用此程序的执行码密钥对临时密钥进行加密获得的第三数值的加密上下文信息。

11. 根据权利要求 10 所述的微处理器, 其中重新启动单元利用秘密密钥由包含在加密上下文信息内的第二数值解密获得第一临时密



钥，并利用第一解密临时密钥由包含在加密上下文信息内的第一数值解密获得指明执行状态的信息，同时利用该程序的执行码密钥由包含在加密上下文信息内的第三数值解密获得第二临时密钥，然后只在第一解密的临时密钥与第二解密的临时密钥一致时，重新启动此程序的执行。

12. 根据权利要求1所述的微处理器，该微处理器进一步包括：

执行状态存储单元，用于存储当前执行程序的执行状态；以及

执行状态初始化单元，被进行配置以在此程序被中断后而在另一个程序开始之前，将执行状态存储单元的内容初始化为规定数值或将执行状态存储单元的内容加密。

13. 根据权利要求1所述的微处理器，该微处理器进一步包括：

密钥读取单元，被进行配置以从外部存储器读出被事先利用公开密钥加密的各程序的执行码密钥；以及

密钥解密单元，被进行配置以利用秘密密钥解密通过密钥读取单元读出的执行码密钥；

其中解密单元利用作为解密密钥的执行码密钥解密各程序。

14. 根据权利要求1所述的微处理器，该微处理器进一步包括：

执行状态存储单元，用于存储当前执行程序的执行状态和将被当前执行程序处理的数据的加密属性；以及

数据加密单元，被进行配置以根据存储在执行状态存储单元的加密属性对将由当前执行程序处理的数据进行加密。

15. 根据权利要求1所述的微处理器，该微处理器进一步包括：

执行状态存储单元，用于存储当前执行程序的执行状态、将被当前执行程序处理的数据的加密属性以及用于规定加密属性的加密属性规定信息；

相关信息写入单元，被进行配置以将涉及加密属性规定信息并含有利用秘密密钥获得的签名的相关信息写入外部存储器；

相关信息读出单元，被进行配置以根据将由当前执行程序引用的数据的地址从外部存储器读出相关信息；